

REMARKS

This application has been reviewed in light of the Office Action dated July 19, 2007. Claims 1, 3, 6-10, 12, 15-19, 21, 24-27, 30-34, 36-41, and 57-59 are pending in this application. Claims 1, 10, 19, 32-34, and 36-41, the independent claims, have been amended to define more clearly what Applicants regard as their invention. Favorable reconsideration is requested.

Claims 1, 3, 6, 10, 12, 15, 19, 21, 24, 31-34, 36-41, and 57-59 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,889,952 (*Hunnicut**t et al.*) in view of U.S. Patent No. 6,971,023 (*Makinson et al.*), in view of U.S. Patent No. 6,920,475 (*Klots et al.*), in view of U.S. Patent No. 7,136,903 (*Phillips et al.*); Claims 7-9, 16-18, and 25-27, as being obvious from *Hunnicut**t et al.* in view of *Makinson et al.*, *Klots et al.*, and *Phillips et al.*, and further in view of U.S. Patent No. 5,550,968 to *Miller et al.*; and Claim 30, as being obvious from *Hunnicut**t et al.* in voew of *Makinson et al.*, *Klots et al.*, and *Phillips et al.*, and further in view of U.S. Patent Application Publication No. US 2003/0028653 to *New, J.*.

Claim 1 is directed to an information processing method of controlling access to computer resource(s) managed by an operating system in a computer, wherein the method is implemented by a specific resource management program located between an operating system and an application. The method includes a storing step of storing a management table in a storage medium, wherein the management table provides, for each computer resource managed by the operating system, access right information representing

access rights for outputting each computer resource to another computer resource, and conditions under which the access right is validated. The method also includes an interception step of intercepting an operation request for a first computer resource from a process, before the operation request is transferred to the operating system, and if the process holds the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource. The method further includes a determination step of monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource, retrieving from the management table access right information of the registered computer resource and access right information of the second computer resource, and determining whether the registered process has an access right for outputting the registered computer resource to the second computer resource based on the access right information retrieved from the management table. The method also includes a processing step of, if it is determined in the determination step that the registered process has the access right for outputting the registered computer resource to the second computer resource, transferring the operation request to the operating system and returning a result from the operating system to the registered process. In addition, the method includes a denial step of denying the operation request, if it is determined in the determination step that

the registered process does not have the access right for outputting the registered computer resource to the second computer resource.

Among other notable features of Claim 1 are an information processing method of controlling access to computer resource(s) managed by an operating system in a computer, the method being implemented by a specific resource management program located between the operating system and an application, the method including (1) an interception step of intercepting an operation request for a first computer resource from a process, before the operation request is transferred to the operating system, and if the process holds the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource, and (2) a determination step, including monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource.

Hunnicuttt et al. is directed to an access-check system for a network server. The Office Action, at pages 4 and 5, states that *Hunnicuttt et al.* “fails to teach intercepting an operation request for a first computer resource from a process, before the operation request is transferred to the operating system, and if the process holds the first computer resource, registering a correspondence between the process and the first computer resource

in a storage medium resulting in a registered process and a registered computer resource . . .”, as recited by Claim 1.

Makinson et al., as understood by Applicants, is directed to a system for scanning computer files for unwanted properties. The Office Action states, at page 5, that *Makinson et al.* teaches scanning access requests prior to servicing by an operating system, and cites column 4, lines 23-45 thereof. However, in the cited portion, *Makinson et al.* states that “[w]ithin the operating system file service 4, the file access requests are intercepted and redirected to an anti-virus system 8.” (Emphasis added.)

Nothing has been found in *Makinson et al.* that would teach or suggest “an interception step of intercepting an operation request for a first computer resource from a process, before the operation request is transferred to the operating systems,” as recited by Claim 1. (Emphasis added.)

The Office Action, at page 5, concedes that *Hunnicuttt et al.* in view of *Makinson et al.* “fails to teach if the process holds the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource”, as recited in Claim 1.

However, the Office Action cites *Klots et al.* as teaching this feature.

Klots et al., as understood by Applicants, is directed to a communication architecture for a distributed computing environment. *Klots et al.* discusses a table that includes entries of resource data maintained by a system, wherein each entry specifies a server node with which the entry is associated and data that specifies services and resources

provided by and/or available on the server node. (See col. 6, lines 21-32 of that patent.)

Apparently, these servers nodes manage a fixed relation between the services and/or resources and the server node itself.

However, the method of Claim 1, in stark contrast, recites registering a correspondence between the process and a computer resource, when the process holds the computer resource. In other words, a relation between the process and the computer resource, which is dynamically changed based on the target of the process, is managed in the method of Claim 1. Even if, assuming *arguendo*, the computer resource of Claim 1 were deemed to be a server node as discussed in *Klots et al.*, *Klots et al.* merely discusses that each server node registers services and resources available on the server itself. That is, the *Klots et al.* server node merely manages a fixed relation between the services and/or resources and the server node itself.

The Office Action, at page 6, concedes that *Hunnicuttt et al.*, *Makinson et al.*, and *Klots et al.* fail to teach “monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource,” as recited in Claim 1.

In this regard, the Office Action, at page 6, cites *Phillips et al.*

Phillips et al., as understood by Applicants, relates to a multi-user shared file access service provided over a wide area network. Apparently, *Phillips et al.* discusses that a file server checks access rights of a client node by using *an operating system* installed

on the file server to control continuing or inhibiting of a process in exchanging access requests and responses between the file server and the client node.

However, the method of Claim 1, in stark contrast, recites controlling access to computer resource(s) managed by an operating system in a computer, wherein the method is implemented by a specific resource management program located between the operating system and an application, instead of the operating system. Accordingly, access of a process independent from the operating system can be controlled in the method of Claim 1.

Nothing in *Hunnicuttt et al.*, *Makinson et al.*, *Klots et al.*, and *Phillips et al.*, whether considered either separately or in any permissible combination (if any) would teach or suggest an information processing method of controlling access to computer resource(s) managed by an operating system in a computer, the method being implemented by a specific resource management program located between the operating system and an application, the method including (1) an interception step of intercepting an operation request for a first computer resource from a process, before the operation request is transferred to the operating system, and if the process holds the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource, and (2) a determination step, including monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation

requests, considered together, has the effect of outputting the registered computer resource to a second computer resource, as recited in Claim 1.

Accordingly, Claim 1 is seen to be clearly allowable over *Hunnicuttt et al.*, *Makinson et al.*, *Klots et al.*, and *Phillips et al.*, whether considered either separately or in any permissible combination (if any).

Independent Claims 10, 19, 32-34, and 36-41 recite features similar in many relevant respects to those discussed above with respect to Claim 1 and therefore are also believed to be patentable over *Hunnicuttt et al.*, *Makinson et al.*, *Klots et al.*, and *Phillips et al.* for at least the reasons discussed above.

A review of the other art of record has failed to reveal anything which, in Applicants' opinion, would remedy the deficiencies of the art discussed above, as a reference against the independent claims herein. All of the independent claims are therefore believed patentable over the cited art.

The other claims in this application are each dependent from one or another of the independent claims discussed above and are therefore believed patentable for the same reasons. Since each dependent claim is also deemed to define an additional aspect of the invention, however, the individual reconsideration of the patentability of each on its own merits is respectfully requested.

CONCLUSION

In view of the foregoing amendments and remarks, Applicants respectfully request favorable reconsideration and early passage to issue of the present application.

Applicants' undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our below listed address.

Respectfully submitted,

/Raymond A. DiPerna/
Raymond A. DiPerna
Attorney for Applicants
Registration No.: 44,063

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

FCBS_WS 1929523_1.DOC